Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US05/001428

International filing date: 14 January 2005 (14.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/536,824
Filing date: 15 January 2004 (15.01.2004)

Date of receipt at the International Bureau: 31 March 2005 (31.03.2005)

Rémark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

1299586

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

March 22, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: ***60/536,824***
FILING DATE: ***January 15, 2004***
RELATED PCT APPLICATION NUMBER: ***PCT/US05/01428***

Certified by

Jon W. Dudas

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

PTO/SB/16 (08-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. EV226792948US

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Paul	OOMMEN	Irving, Texas USA

Additional inventors are being named on the _____ separately numbered sheets attached hereto

TITLE OF THE INVENTION (500 characters max)

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☑ Customer Number: 26343

OR

☐ Firm or Individual Name					
Address					
Address					
City		State		Zip	
Country		Telephone		Fax	

ENCLOSED APPLICATION PARTS *(check all that apply)*

☑ Specification *Number of Pages* 12 ☐ CD(s), Number _____

☑ Drawing(s) *Number of Sheets* 2 ☐ Other (specify) _____

☐ Application Data Sheet. See 37 CFR 1.76

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check or money order is enclosed to cover the filing fees.

☑ The Director is herby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 50-0270

☐ Payment by credit card. Form PTO-2038 is attached.

FILING FEE Amount ($): 160.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☑ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE _____

TYPED or PRINTED NAME Steven A. Shaw

TELEPHONE 972-894-6173

Date January 15, 2004

REGISTRATION NO. 39,368 *(if appropriate)*

Docket Number: NC17713P

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop Provisional Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

15866 U.S.PTO 011504

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($) 160.00

Complete if Known	
Application Number	Not Assigned
Filing Date	01/15/2004
First Named Inventor	OOMMEN
Examiner Name	N/A
Art Unit	N/A
Attorney Docket No.	NC17713P

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☑ Deposit Account:

Deposit Account Number: 50-0270

Deposit Account Name: NOKIA INC.

The Director is authorized to: *(check all that apply)*

☑ Charge fee(s) indicated below ☑ Credit any overpayments

☑ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	160.00

SUBTOTAL (1) ($) 160.00

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

		Extra Claims		Fee from below	Fee Paid
Total Claims		-20** =		x	=
Independent Claims		- 3** =		x	=
Multiple Dependent					=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($)

SUBMITTED BY				(Complete *(if applicable)*)	
Name (Print/Type)	Steven A. Shaw	*Registration No. (Attorney/Agent)*	39,368	*Telephone*	972-894-6173
Signature				*Date*	1/15/04

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Express Mail No.:EV226792948US

Attorney Docket No. NC17713P
Provisional Application Papers of Paul Oommen

METHOD FOR A-KEY EXCHANGE AND UPDATING CRITICAL CDMA PARAMETERS

BACKGROUND

[0001] This invention pertains generally to communication of systems and more particularly to IP Based Over-the-Air Device Management of mobile stations.

[0002] There are some critical parameters used in Code Division Multiple Access (CDMA) mobile stations (MS), which are essential for signaling and data communication. One such parameter is the 128-bit Authentication Key (A-Key) (64 bit in legacy MS). The A-key is different from other parameters. It is known only to the Authentication Center (AC) and the MS. While other parameters may be updated using normal request response (IS-683 or IP based) messages, parameters like A-Key require a secure method. IS-683 (IS-683-A and later revisions) defines the method for updating A-Key in IS-95/ cdma2000 devices using signaling messages. But an IP based method for A-Key update is not defined. Purpose of embodiments of this invention is to describe an IP based method for A-Key update, as well as other critical parameters in cdma2000 mobile stations.

[0003] The invention is related to the IP Based Over-the-Air Device Management (IOTA-DM) work item in the 3GPP2 TSG-S standard specification.

[0004] In CDMA systems, a special parameter called Authentication Key (A-Key) is used for the generation of Shared Secret Data (SSD). The SSD is used for the encryption of data sent in the physical layer as well as layer 2 signaling. The A-Key is assigned to the MS in a secure way. A method for updating A-Key is described in IS-683. But this

procedure uses signaling messages for updating A-Key and hence limited to the specific implementation.

[0005] There is significant interest in IP based methods for managing mobile stations over-the-air (OTA). Corresponding standards work is progressing in OMA and 3GPP2. Current versions of IP based protocols do not define a method for A-Key exchange.

SUMMARY

[0006] A method according to an embodiment of this invention provides an IP based method for A-Key exchange, and updating other critical parameters in cdma2000 mobile stations and beyond.

[0007] These and other features, aspects, and advantages of embodiments of the present invention will become apparent with reference to the following description in conjunction with the accompanying drawings. It is to be understood, however, that the drawings are designed solely for the purposes of illustration and not as a definition of the limits of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Figure 1 is a session diagram illustrative of an embodiment of the invention wherein there is OTAF and IS-683 client in the mobile station.

[0009] Figure 2 is a session diagram illustrative of an embodiment of the invention wherein the mobile station does not Support IS-683 Client.

DETAILED DESCRIPTION

[0010] An embodiment of this invention provides a method for updating A-Key in CDMA mobile stations using the DM framework. The method can be used for the update of other critical parameters in the MS, which are not accessible using normal methods. A-Key is a critical parameter, which is known only to the Authentication Center (AC) and the mobile station. In CDMA mobile stations, the A-Key is updated using over-the-air (OTA) methods.

[0011] Figure 1 is a session diagram illustrative of an embodiment of the invention wherein there is OTAF and IS-683 client in the mobile station. Entities which may participate in various parts of session 100 are A-Key IS-683 Client 110, Mobile Station Management Tree 120, Mobile Station Device Management Client 130, Over The Air Device Management Server 140, Over The Air Function (OTAF) Server 150. The method comprises the following when there is OTAF and IS683 client in the mobile station.

1001. The IS-683 Server in the network initiates the A-Key update procedure by issuing a "Key Request Message" as described in IS-683.

1002. The OTA-DM Server intercepts the message and buffers it. The Server then sends a notification to the MS DM client. This message is package #0 in the DM protocol, which acts as a trigger. This trigger can carry the identification "A-KET GEN", by which the MS DM Client identifies it as a trigger to begin the updating of A-Key.

1003. The MS DM Client responds with "MS Capability Message". This is a standard package #1 message in the DM protocol, but for the specific purpose of A-Key update, this message will carry new parameters to identify the capabilities of the MS. The parameter

would include if the MS supports scenario 2.1 or 2.2 described in this document.

1004. After receiving the "MS Capability Message", the IOTA-DM server knows which scenario to be followed, i.e. whether the subsequent messaging is for scenario 2.1 or scenario 2.2 described in this document. If it is scenario 2.1, the IOTA-DM Server creates a new message "IOTA-DM Key Request Message by encapsulating the "Key Request message" originated from the IS-683 server as well as additional commands. One additional command is the standard "Exec" command in the DM protocol. But here the "Exec" command is executed on a special node in the MS Management Tree. This node corresponds to the A-Key in the MS. Since A-Key is stored only in the MS permanent storage or in the R-UIM/UICC, this node in the management tree is a dummy node, which does not store the value of A-Key, but points to process which the "Exec" command should execute upon receiving the "IOTA-DM Key Generation Request Message". In scenario 2.1, this process is the IS-683 client running in the MS. The "Key Request Message" received at the IOTA-DM Client can be stored in a temporary leaf node of the A-Key node, from where the invoked IS-683 client can access it.

1005. On receiving the "IOTA-DM Key Request Message" the MS DM Client executes the commands specified in the message. This involves executing the "Exec" command on the A-Key node in the Management Tree, which results in passing the encapsulated "Key Generation Request Message" to the IS-683 Client.

1006. The IS-683 Client calculates the MS_RESULT parameter based on the input parameters in the encapsulated message. The algorithm described in section 5.1 of C.S0016 Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, 3GPP2, March 2003 is followed for calculating MS_RESULT.

1007. The IS-683 Client sends the "Key Response Message" which includes the status of the MS_RESULT calculation. If an error occurred, the error code is sent in the response as described in C.S0016 Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, 3GPP2, March 2003.

1008. The "Key Response Message" is intercepted by the IOTA-DM Client and encapsulated in a DM protocol message called "IOTA-DM Key Gen. Response" Message. One way is to store the "Key Response Message" in a temporary leaf node associated with the A-Key node in the management tree from where the IOTA-DM client can access it for encapsulation.

1009. The IOTA-DM Client sends the encapsulated "IOTA-DM Key Response Message" to the IOTA-DM Server.

1010. The IOTA-DM server forwards the encapsulated message to the IS-683 Server.

1011. The IS-683 Server calculates the BS_RESULT following the algorithm in section 5.2 of C.S0016 Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, 3GPP2, March 2003 and sends it to the MS in the "Key Generation Request message".

1012. The IOTA-DM Server encapsulates the "Key Generation Request Message" in a DM Protocol message and sends it to the MS IOTA-DM Client in the "IOTA-DM Key Generation Request". This message also carries the "Exec" command to invoke the IS-683 client.

1013. Executing the "Exec" command results in invoking the MS IS-683 client process.

1014. The IS-683 client calculates the A-Key from the BS_RESULT.

1015. The IS-683 Client now sends the MS_RESULT calculated in step 6 in the "Key Generation Response Message. The message is encapsulated in the IOTA-DM message. This can be achieved by the IS-683 client first storing the message in a temporary leaf node of the A-Key node and then the IOTA-DM client accessing it.

1016. The IOTA-DM server forwards the MS_RESULT to the IS-683 Server.

1017. The IS-683 server computes the A-Key and issues a commit message.

1018. The IOTA-DM server directs the commit message to the MS IOTA-DM client.

1019. The MS IOTA-DM client forwards this message to the IS-683 client. On receiving the commit the IS-683 Client stores the A-Key in a permanent memory.

1020. The IS-683 client now sends a "Commit response".

1021. The commit response is encapsulated in the "IOTA-DM Commit Response".

1022. The IOTA-DM server forwards the encapsulated message to the IS-683 server.

[0012] The IS-683 server can now update the A-Key in the AC.

[0013] Figure 2 is a session diagram illustrative of an embodiment of the invention wherein the mobile station does not Support IS-683 Client. Entities that may participate in various parts of session 200 are A-Key Client 210, Mobile Station Management Tree 220, Mobile Station IP Based Over-the-Air Device Management Client 230, IP Based Over-the-Air Device Management Server 240, and Authentication. The method

comprises the following when there the mobile station does not support IS-683 client.

2001. The Authentication Center (AC) initiates a trigger to update the A-Key in the MS.

2002. The IOTA-DM server begins a notification-initiated session by sending a notification message with data "A-KEY GEN".

2003. The IOTA-DM client responds with package #1 carrying the MS capability information. This enables the DM Server to tailor the contents according to the capabilities of the device. Step 4. onwards assume that the device is SyncML DM capable.

2004. The IOTA-DM server creates Key Request message and sends it to the MS Client in DM Protocol [2] message. The message includes the input parameters mentioned in section 5.1.2 of C.S0016 Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, 3GPP2, March 2003.

2005. The IOTA-DM client executes the Exec command in the message. The Exec command carries information about the process to be invoked for calculating A-Key. The process can be integrated to the IOTA-DM client, in which case a separate A-Key Client is not required. The parameters from the message received in step 4 is provided as input parameters to the A-Key client.

2006. The A-key client computes the MS_RESULT parameter.

2007. The result code is send in the Key Response message.

2008. The IOTA-DM Server computes the BS_RESULT (See procedures in 5.2.1 of C.S0016 Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, 3GPP2, March 2003).

2009. The IOTA-DM Server sends the BS_RESULT to the MS client in a "Key Generation Request Message".

2010. The IOTA-DM client passes the parameters to the A-Key Client.

2011. The A-Key client computes the A-KEY following the algorithm described in section 5.1 of C.S0016 Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, 3GPP2, March 2003, based on input parameters in step 4 and the BS_RESULT from step 9. The value can be stored in a temporary location in the management tree.

2012. The IOTA-DM Client sends the "Key Generation Response Message". MS_RESULT computed in step 6 is send in this message to the IOTA-DM Server.

2013. The IOTA-DM Server computes the A-Key based on MS_RESULT, following the algorithm in section 5.2 of C.S0016 Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, 3GPP2, March 2003.

2014. The DM Server sends a "Commit Message" to the IOTA-DM Client.

2015. On receipt of the commit request, the IOTA-DM client invokes the A-Key client to store the A-Key stored in temporary node of the management tree to the permanent memory A-KEYp and removes the A-Key from temporary storage.

2016. The IOTA-DM client sends the status of in the commit response message.

2017. The IOTA-DM server updates the A-Key to the Authentication Center (AC).

[0014] Although described in the context of particular embodiments, it will be apparent to those skilled in the art that a number of modifications and various changes to these teachings may occur. Thus, while the invention has been particularly shown and described with respect to one or more preferred embodiments thereof, it will be understood by those skilled in the art that certain modifications or changes, in form and shape, may be made therein without departing from the scope and spirit of the invention as set forth above.

ABSTRACT

[0015] A method according to an embodiment of this invention provides an IP based method for A-Key exchange, and updating other critical parameters in cdma2000 mobile stations and beyond.

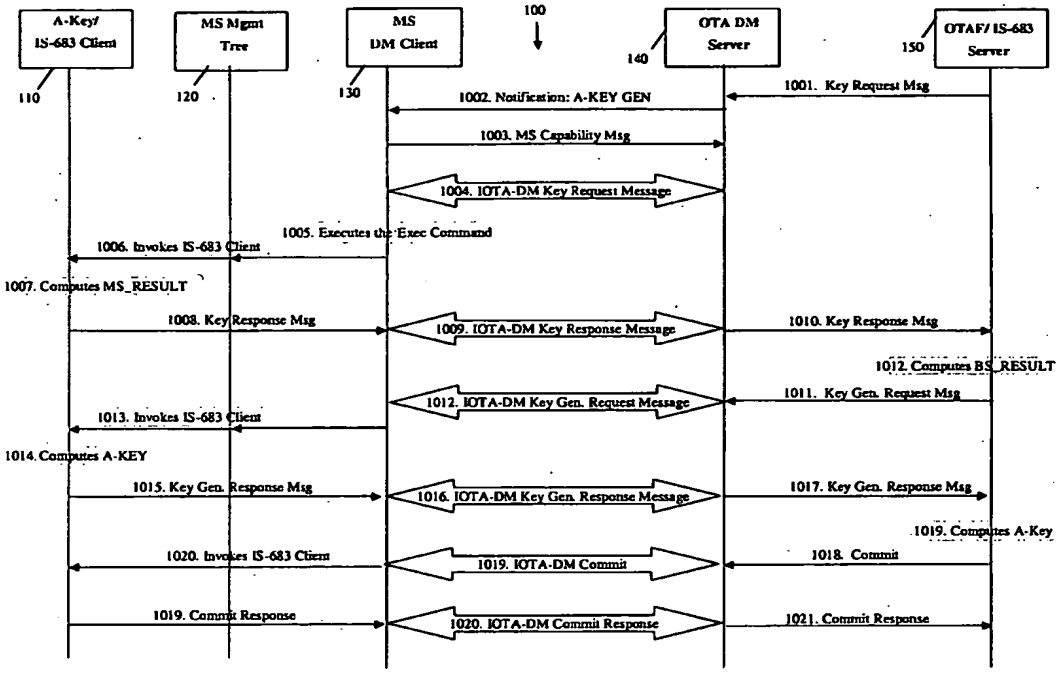
A-Key/ IS-683 Client
MS Mgmt Tree
MS DM Client
100
OTA DM Server
OTAF/ IS-683 Server
110
120
130
140
150
1001. Key Request Msg
1002. Notification: A-KEY GEN
1003. MS Capability Msg
1004. IOTA-DM Key Request Message
1005. Executes the Exec Command
1006. Invokes IS-683 Client
1007. Computes MS_RESULT
1008. Key Response Msg
1009. IOTA-DM Key Response Message
1010. Key Response Msg
1012. Computes BS_RESULT
1011. Key Gen. Request Msg
1012. IOTA-DM Key Gen. Request Message
1013. Invokes IS-683 Client
1014. Computes A-KEY
1015. Key Gen. Response Msg
1016. IOTA-DM Key Gen. Response Message
1017. Key Gen. Response Msg
1019. Computes A-Key
1020. Invokes IS-683 Client
1019. IOTA-DM Commit
1018. Commit
1019. Commit Response
1020. IOTA-DM Commit Response
1021. Commit Response

FIGURE 1

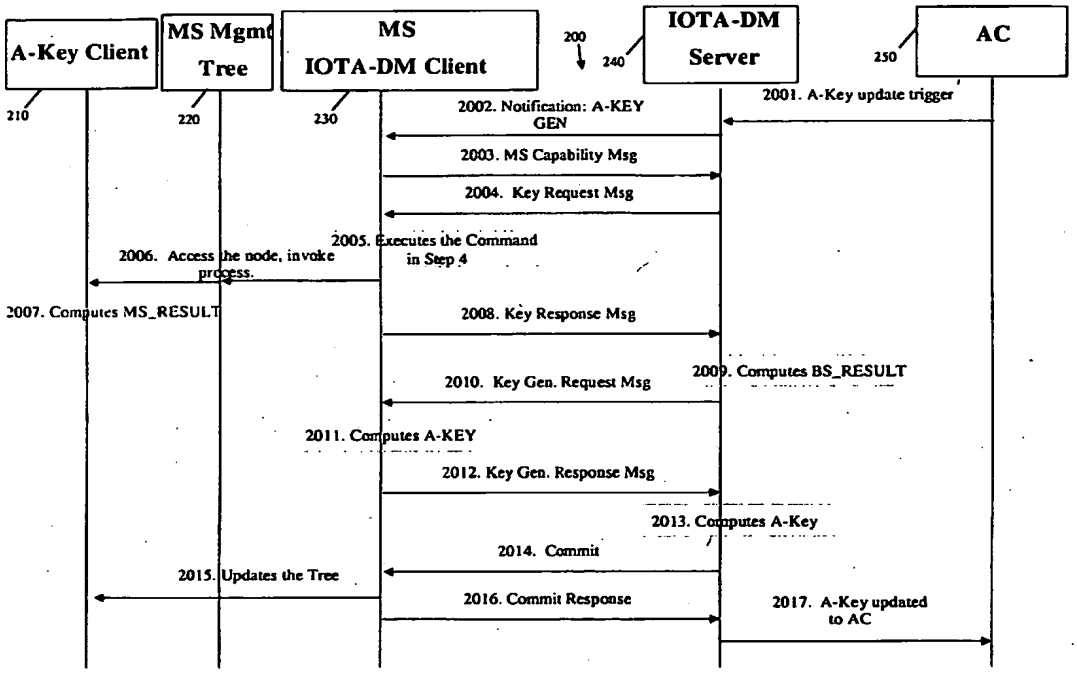
A-Key Client
MS Mgmt Tree
MS IOTA-DM Client
200
IOTA-DM Server
AC
210
220
230
240
250
2001. A-Key update trigger
2002. Notification: A-KEY GEN
2003. MS Capability Msg
2004. Key Request Msg
2005. Executes the Command in Step 4
2006. Access the node, invoke process.
2007. Computes MS_RESULT
2008. Key Response Msg
2009. Computes BS_RESULT
2010. Key Gen. Request Msg
2011. Computes A-KEY
2012. Key Gen. Response Msg
2013. Computes A-Key
2014. Commit
2015. Updates the Tree
2016. Commit Response
2017. A-Key updated to AC

FIGURE 2